

1 WILLIAM L. ANTHONY (State Bar No. 106908)  
2 ERIC L. WESENBERG (State Bar No. 139696)  
3 MARK R. WEINSTEIN (State Bar No. 193043)  
4 ORRICK, HERRINGTON & SUTCLIFFE, LLP  
5 1000 Marsh Road  
6 Menlo Park, CA 94025  
7 Telephone: (650) 614-7400  
8 Facsimile: (650) 614-7401

9 STEVEN ALEXANDER (admitted *Pro Hac Vice*)  
10 KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)  
11 JAMES E. GERINGER (admitted *Pro Hac Vice*)  
12 JOHN D. VANDENBERG  
13 KLARQUIST SPARKMAN, LLP  
14 One World Trade Center, Suite 1600  
15 121 S.W. Salmon Street  
16 Portland, OR 97204  
17 Telephone: (503) 226-7391  
18 Facsimile: (503) 228-9446

19 Attorneys for Defendant and Counterclaimant,  
20 MICROSOFT CORPORATION

21 UNITED STATES DISTRICT COURT  
22 NORTHERN DISTRICT OF CALIFORNIA  
23 OAKLAND DIVISION

24 INTERTRUST TECHNOLOGIES  
25 CORPORATION, a Delaware corporation,  
26 Plaintiff,

27 v.

28 MICROSOFT CORPORATION, a  
Washington corporation,  
Defendant.

MICROSOFT CORPORATION, a  
Washington corporation,  
Counterclaimant,

v.

INTERTRUST TECHNOLOGIES  
CORPORATION, a Delaware corporation,  
Counter Claim-Defendant.

CASE NO. C01-1640 SBA

**MICROSOFT CORPORATION'S  
PATENT LOCAL RULE 4-1(a)  
STATEMENT (LIMITED TO "MINI-  
MARKMAN" CLAIMS)**

1 Pursuant to Patent Local Rule 4-1(a), Microsoft submits below the claim terms, phrases,  
2 and clauses of the twelve selected "Mini-Markman" patent claims that Microsoft presently  
3 submits, subject to discussions with InterTrust, should be construed by the Court, in addition to  
4 construing each claim as a whole.

5  
6 Set forth in Section A, below, is a list of individual claim terms that Microsoft presently  
7 submits, subject to discussions with InterTrust, should be construed by the Court. Individual  
8 claim terms should be construed wherever they are found in these twelve claims.

9 Set forth in Section B, below, are the phrases and clauses that Microsoft presently  
10 submits, subject to discussions with InterTrust, should be construed by the Court. The claim  
11 phrases and clauses that Microsoft presently submits, subject to discussions with InterTrust,  
12 should be governed by 35 U.S.C. § 112(6), are identified in Section B by double underlining.

13  
14 Many of these claim terms, phrases and clauses are indefinite and otherwise improper  
15 under 35 U.S.C. § 112(2), and Microsoft reserves all rights to assert those defects as to each of  
16 these claim terms, phrases and clauses.

17 The grouping of individual claim terms below is for convenience only and does not imply  
18 any particular connection, or lack of connection, between any terms.

19 **A. Individual Claim Terms**

- 20  
21 • a digital file, digital file  
22 • access, accessed, access to, accessing  
23 • addressing  
24 • allowing, allows  
25 • applying . . . in combination  
26 • arrangement  
27 • aspect  
28 • associated with  
• authentication  
• authorization information, authorized, not authorized  
• budget control, budget

- 1 • can be
- 2 • capacity
- 3 • clearinghouse
- 4 • compares, comparison
- 5 • component assembly
- 6 • contain, contained, containing
- 7 • control (n.), controls (n.)
- 8 • controlling, control (v.)
- 9 • copied file
- 10 • copy, copied, copying
- 11 • copy control
- 12 • creating, creation
- 13 • data item
- 14 • derive, derives
- 15 • descriptive data structure
- 16 • designating
- 17 • device class
- 18 • digital signature, digitally signing
- 19 • entity, entity's control
- 20 • environment
- 21 • executable programming, executable
- 22 • execution space, execution space identifier
- 23 • generating
- 24 • govern, governed, governed item, governing
- 25 • halting
- 26 • host processing environment
- 27 • identifier, identify, identifying
- 28 • including
- information previously stored
- integrity programming
- key
- load module
- machine check programming
- metadata information
- opening secure containers
- operating environment, said operating environment
- organization, organization information, organize
- portion
- prevents
- processing environment

- 1 • protected processing environment
- 2 • protecting
- 3 • record
- 4 • required
- 5 • resource processed
- 6 • rule
- 7 • secure
- 8 • secure container, secure containers
- 9 • secure container governed item
- 10 • secure container rule
- 11 • secure database
- 12 • secure execution space
- 13 • secure memory, memory
- 14 • secure operating environment, said operating environment
- 15 • securely applying
- 16 • securely assembling
- 17 • securely processing
- 18 • securely receiving, securely receiving . . . a control
- 19 • security
- 20 • security level, level of security
- 21 • specific information, specified information
- 22 • tamper resistance
- 23 • tamper resistant barrier
- 24 • tamper resistant software
- 25 • tampering
- 26 • use
- 27 • validity
- 28 • virtual distribution environment

21 B. Claim Phrases and Clauses

22 '193:1

- 23 • receiving a digital file including music
- 24 • a budget specifying the number of copies which can be made of said digital file
- 25 • controlling the copies made of said digital file
- 26 • determining whether said digital file may be copied and stored on a second device based on at least said copy control
- 27 • if said copy control allows at least a portion of said digital file to be copied and stored on a second device
- 28 • copying at least a portion of said digital file

- 1 • transferring at least a portion of said digital file to a second device
- 2 • storing said digital file

3 '193:11

- 4 • receiving a digital file
- 5 • determining whether said digital file may be copied and stored on a second device based on said first control
- 6 • identifying said second device
- 7 • whether said first control allows transfer of said copied file to said second device
- 8 • said determination based at least in part on the features present at the device
- 9 • if said first control allows at least a portion of said digital file to be copied and stored on a second device
- 10 • copying at least a portion of said digital file
- 11 • transferring at least a portion of said digital file to a second device
- 12 • storing said digital file

13 '193:15

- 14 • receiving a digital file
- 15 • an authentication step comprising:
- 16 • accessing at least one identifier associated with a first device or with a user of said first device
- 17 • determining whether said identifier is associated with a device and/or user authorized to store said digital file
- 18 • storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized
- 19 • storing information associated with said digital file in a secure database stored on said first device, said information including at least one control
- 20 • determining whether said digital file may be copied and stored on a second device based on said at least one control
- 21 • if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,
- 22 • copying at least a portion of said digital file
- 23 • transferring at least a portion of said digital file to a second device
- 24 • storing said digital file

25 '193:19

- 26 • receiving a digital file at a first device
- 27 • establishing communication between said first device and a clearinghouse located at a location remote from said first device
- 28 • using said authorization information to gain access to or make at least one use of said first digital file
- 29 • including using said key to decrypt at least a portion of said first digital file

- 1 • receiving a first control from said clearinghouse at said first device
- 2 • storing said first digital file in a memory of said first device
- 3 • using said first control to determine whether said first digital file may be copied and stored on
- 4 • if said first control allows at least a portion of said first digital file to be copied and stored on
- 5 • copying at least a portion of said first digital file
- 6 • transferring at least a portion of said first digital file to a second device including a memory
- 7 • storing said first digital file portion

8 '683:2

- 9 • user controls
- 10 • the first secure container having been received from a second apparatus
- 11 • an aspect of access to or use of
- 12 • the first secure container rule having been received from a third apparatus different from said
- 13 • hardware or software used for receiving and opening secure containers
- 14 • said secure containers each including the capacity to contain a governed item, a secure
- 15 • container rule being associated with each of said secure containers
- 16 • protected processing environment at least in part protecting information contained in said
- 17 • protected processing environment from tampering by a user of said first apparatus
- 18 • hardware or software used for applying said first secure container rule and a second secure
- 19 • container rule in combination to at least in part govern at least one aspect of access to or use
- 20 • of a governed item contained in a secure container
- 21 • hardware or software used for transmission of secure containers to other apparatuses or for the
- 22 • receipt of secure containers from other apparatuses.

23 '721:1

- 24 • digitally signing a first load module with a first digital signature designating the first load
- 25 • module for use by a first device class
- 26 • digitally signing a second load module with a second digital signature different from the first
- 27 • digital signature, the second digital signature designating the second load module for use by a
- 28 • second device class having at least one of tamper resistance and security level different from
- 29 • the at least one of tamper resistance and security level of the first device class
- 30 • distributing the first load module for use by at least one device in the first device class
- 31 • distributing the second load module for use by at least one device in the second device class

32 '721:34

- 33 • arrangement within the first tamper resistant barrier
- 34 • prevents the first secure execution space from executing the same executable accessed by a
- 35 • second secure execution space having a second tamper resistant barrier with a second security
- 36 • level different from the first security level

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

'861:58

- creating a first secure container
- including or addressing . . . organization information . . . desired organization . . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container
- at least in part determine specific information required to be included in said first secure container contents
- rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents

'891:1

- resource processed in a secure operating environment at a first appliance
- securely receiving a first entity's control at said first appliance
- securely receiving a second entity's control at said first appliance
- securely processing a data item at said first appliance, using at least one resource
- securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item

'900:155

- first host processing environment comprising
- said mass storage storing tamper resistant software
- designed to be loaded into said main memory and executed by said central processing unit
- said tamper resistant software comprising: . . . one or more storage locations storing said information
- derives information from one or more aspects of said host processing environment,
- one or more storage locations storing said information
- information previously stored in said one or more storage locations
- generates an indication based on the result of said comparison
- programming which takes one or more actions based on the state of said indication
- at least temporarily halting further processing

'912:8

- identifying at least one aspect of an execution space
- required for use and/or execution of the load module
- said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security
- checking said record for validity prior to performing said executing step

1 '912:35

- 2 • received in a secure container  
3 • said component assembly allowing access to or use of specified information  
4 • said first component assembly specified by said first record

5 Dated: November 8, 2002

6  
7 By: 

8 WILLIAM L. ANTHONY  
9 ERIC L. WESENBERG  
10 MARK R. WEINSTEIN  
11 ORRICK HERRINGTON & SUTCLIFFE, LLP  
12 1000 Marsh Road  
13 Menlo Park, CA 94025  
14 Telephone: (650) 614-7400

15 STEVEN ALEXANDER  
16 KRISTIN L. CLEVELAND  
17 JAMES E. GERINGER  
18 JOHN D. VANDENBERG  
19 KLARQUIST SPARKMAN, LLP  
20 One World Trade Center, Suite 1600  
21 121 S.W. Salmon Street  
22 Portland, OR 97204  
23 Telephone: (503) 226-7391

24 Attorneys for Defendant  
25 MICROSOFT CORPORATION

26 Of Counsel:

27 T. Andrew Culbert, Esq.  
28 One Microsoft Way  
Building 8  
Redmond, WA 98052-6399  
Phone: 425-882-8080



